

IN THE CLAIMS

Please amend claims 1-8, 12-15, 18, and 21 as indicated below.

1. (Currently Amended) A computer implemented method comprising:  
in response to a request for establishing a generic routing encapsulation (GRE) tunnel received at a first network element, the first network element determining a set of endpoints for a generic routing encapsulation (GRE) the requested GRE tunnel based on the request;  
determining a key, the key corresponding to a virtual private network (VPN);  
dynamically establishing the GRE tunnel with the set of endpoints and the key  
between the first network element and a second network element, the second network element being identified by the set of endpoints; and  
processing a set of GRE traffic for the VPN within the established GRE tunnel between the first and second network elements over a network provided by a network provider.
  
2. (Currently Amended) The computer implemented method of claim 1 wherein the set of points comprise a first value indicating a first virtual router, the first virtual router corresponding to the VPN, a second value indicating a second virtual router, a third value indicating a third virtual router, the second and third virtual routers corresponding to a backbone, and a fourth value indicating a fourth virtual router, the fourth virtual router corresponding to the VPN, the set of endpoints comprises a first set of endpoints, wherein the method further comprises:

the first network element determining the first set of endpoints based on an ID of the requested GRE tunnel, the first set of endpoints identifying the second network element; and

the first network element transmitting the first set of endpoints and the key to the second network element to enable the second network element to respond in establishing the GRE tunnel with the first network element.

3. (Currently Amended) The computer implemented method of claim 1 wherein dynamically establishing the GRE tunnel comprises: 2, wherein the set of endpoints further comprises a second set of endpoints, wherein the method further comprises:
- the first network element determining the second set of endpoints based on the first set of endpoints and the key, the first and second sets of endpoints identifying a first and second virtual routers of the first network element, the first virtual router interfacing with a first site of an entity from which the request is originated and the second virtual router interfacing with the second network element; and
- directing network traffic between the first and second virtual routers, where the second virtual router exchanges the network traffic with the second network element via the GRE tunnel.
- ~~establishing a first subset of the set of endpoints for entering and exiting the VPN; and establishing an initiation point and a termination point for the GRE tunnel with a second subset of the set of endpoints.~~

4. (Currently Amended) A computer implemented method comprising:

determining a first set of endpoints for a generic routing encapsulation (GRE) tunnel; determining a key, the key corresponding to a virtual private network (VPN); using the key and the set of endpoints to determine a second set of endpoints for the VPN; establishing the GRE tunnel with the set of attributes; and processing a set of traffic for the VPN. The computer implemented method of claim 3, wherein the set of endpoints further comprises a third set of endpoints, wherein the method further comprises:

receiving at a third virtual router of the second network element the first set of endpoints and the key received from the first network element, the third virtual router interfacing the second network element with the first network element via the GRE tunnel;

the second network element determining the third set of endpoints based on the first set of endpoints and the key, the third set of endpoints identifying a fourth virtual router interfacing the second network element with a second site of the entity; and

directing the network traffic between the third and fourth virtual routers, where the fourth virtual router exchanges the network traffic with the second site of the entity.

5. (Currently Amended) The computer implemented method of claim 4 wherein the first set of endpoints comprise a first value indicating a first virtual router, the first virtual router being an initiation point of the GRE tunnel, and a second value indicating a second virtual router, the second virtual router being a termination point for the GRE tunnel. the first

the network element accesses a remote server to determine the first set of endpoints based on the ID of the requested GRE tunnel, wherein in response to the first set of endpoints, the first network element access the remote server to determine the second set of endpoints using the first set of endpoints and the key, and wherein in response to the first set of endpoints and the key received from the first network element, the second network element accesses the remote server to determine the third set of endpoints.

6. (Currently Amended) The computer implemented method of claim 4 wherein the second set of endpoints comprise a first value indicating a first virtual router corresponding to the VPN, and a second value indicating a second virtual router, the second virtual router corresponding to the VPN the entity is a first entity and the first and second sites of the first entity exchange network traffic via a first VPN within the GRE tunnel, wherein the method further comprises establishing a second VPN within the GRE tunnel between a third site and a fourth site of a second entity to enable the third and fourth sites of the second entity to exchange network traffic via the second VPN within the GRE, such that the first and second entities share the GRE tunnel using the first and second VPNs.

7. (Original Currently Amended) The computer implemented method of claim 4-6 wherein the second set of endpoints and the set of attributes are each indexed by the key and the first set of endpoints the remote server comprises a RADIUS, wherein the second and third set of endpoints comprise substantially identical information retrieved from the RADIUS, and wherein the first and second entities are different organizations sharing the first and second network elements to traverse through the network of the network provider.

8. (Currently Amended) A system comprising:

a first network element to determine a key and a first set of endpoints for a generic routing encapsulation (GRE) tunnel, the key corresponding to a virtual private network (VPN), to determine a second set of endpoints for the GRE VPN based on the first set of endpoints and the key, to configure an initiation point of the GRE tunnel based on the first and second sets of endpoints, to transmit a packet having the first set of end points endpoints and the key; and a second network element coupled with the first network element, the second network element to receive the packet, to determine the second set of endpoints for the GRE VPN using the received first set of endpoints and the key, and to establish the GRE tunnel with the first network element using the first and second sets of endpoints.

9. (Original) The system of claim 8 further comprising a third network element, the third network element coupled with the first and the second network element, the third network element to receive a set of data from the first network element and forward the set of data to the second network element, the set of data being for the VPN.

10. (Original) The system of claim 8 wherein the second set of endpoints are indexed by the first set of endpoints and the key.

11. (Original) The system of claim 8 wherein to configure the initiation point comprises to configure one of the second set of endpoints to one of the first set of endpoints.

12. (Currently Amended) An apparatus comprising:

a control engine to retrieve a first set of endpoints corresponding to a generic routing encapsulation (GRE) tunnel based on an ID of the GRE tunnel, to retrieve a second set of endpoints corresponding to the first set of endpoints and a key, the key corresponding to a virtual private network (VPN); and a forwarding engine coupled with the control engine, the forwarding engine to establish an initiation point of the GRE tunnel using the first and second sets of endpoints and to transmit a set of traffic over the GRE VPN with a termination point of the GRE tunnel over a network of a network provider, wherein at least one of the first and second sets of endpoints identifies the termination point of the GRE tunnel.

13. (Currently Amended) The apparatus of claim 11-12 wherein the forwarding engine to host a first and second virtual router, the first virtual router corresponding to one of the first set of endpoints and the second virtual router corresponding to one of the second set of endpoints.

14. (Currently Amended) The apparatus of claim 11-12 wherein the second set of endpoints are indexed by the key and the first set of endpoints.

15. (Currently Amended) An apparatus comprising:

an input/output module to receive a set of data from a network element over a network, the set of data indicating a key and a first of set of endpoints of a

generic routing encapsulation (GRE) tunnel, the key corresponding to a virtual private network (VPN); and

a control engine coupled with the input/output module, the control engine to determine a second set of endpoints for the VPN with the key and the first set of endpoints; and

a forwarding engine coupled with the control engine and the input/output module, the forwarding engine to dynamically establish the GRE tunnel with the network element over the network using the first set of endpoints and the second set of endpoints and to process a set of traffic for the VPN.

16. (Original) The apparatus of claim 15 wherein the second set of endpoints are indexed by the key and the first set of endpoints.

17. (Original) The apparatus of claim 15 wherein to establish the GRE tunnel comprises: to configure one of the second set of endpoints to one of the first set of endpoints; and to indicate the key in a list of keys.

18. (Currently Amended) A machine-readable medium that provides instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

retrieving a first set of endpoints of a generic routing encapsulation (GRE) tunnel with based on a generic routing encapsulation (GRE) tunnel name of the GRE tunnel in response to a request for establishing the GRE tunnel, the first set of endpoints identifying a termination point of the GRE tunnel;

determining a second set of endpoints with the first set of endpoints and a key, the key

corresponding to a virtual private network (VPN);

establishing an initiation point of the GRE tunnel with the first set of endpoints and the  
second set of endpoints;

transmitting the first set of endpoints and the key to the identified termination point to

establish the GRE tunnel with the termination point; and

transmitting a set of traffic over the GRE VPN.

19. (Original) The machine-readable medium of claim 18 wherein the establishing the  
initiation point of the GRE tunnel comprises configuring one of the second set of endpoints to  
one of the first set of endpoints.

20. (Original) The machine-readable medium of claim 18 further comprising:  
receiving a second set of traffic for a second VPN, the second set of traffic indicating  
the GRE tunnel;  
determining a third set of endpoints with a second key and the first set of endpoints,  
the second key corresponding to the second VPN;  
configuring one of the third set of endpoints to one of the first set of endpoints;  
transmitting the second key and the first set of endpoints; and  
transmitting the second set of traffic.

21. (Currently Amended) A machine-readable medium that provides instructions, which  
when executed by a set of one or more processors, cause said set of processors to perform  
operations comprising:

listening for a packet, the packet indicating a first set of endpoints for a generic routing encapsulation (GRE) tunnel and a key, the key corresponding to a virtual private network (VPN);

~~receiving the packet;~~

in response to the packet received from a network element over a network, retrieving a second set of endpoints for the VPN with the first set of endpoints and the key; establishing the GRE tunnel with the network element over the network using the first set of endpoints and the second set of endpoints; and processing a set of traffic over the GRE VPN.

22. (Original) The machine-readable medium of claim 21 wherein establishing the GRE tunnel comprises:

configuring one of the second set of endpoints to one of the first set of endpoints; and maintaining the key in a list of keys.

23. (Original) The machine-readable medium of claim 21 further comprising:

receiving a second packet, the second packet indicating the first set of endpoints and a second key, the second key corresponding to a second VPN;  
retrieving a third set of endpoints with the second key and the first set of endpoints;  
receiving a second set of traffic; and  
forwarding the second set of traffic to one of the third set of endpoints.

24. (Original) The machine-readable medium of claim 21 further comprising:

receiving a second packet, the second packet indicating a second key;

determining that the second key is not in a key list; and  
ensuring that the second packet originated from an interior source.